

⑫ 公開特許公報(A)

昭63-184164

⑪ Int. Cl.⁴G 06 F 15/21
15/30
G 06 K 17/00

識別記号

3 4 0
3 4 0

庁内整理番号

C-7230-5B
7208-5B
T-6711-5B

⑬ 公開 昭和63年(1988)7月29日

審査請求 未請求 発明の数 1 (全5頁)

⑭ 発明の名称 ICカードシステム

⑮ 特 願 昭61-188186

⑯ 出 願 昭61(1986)8月11日

⑰ 発 明 者 横 江 川 光 東京都足立区東綾瀬2-5-2-401

⑱ 出 願 人 横 江 川 光 東京都足立区東綾瀬2-5-2-401

明 細 書

1 発明の名称 ICカードシステム

2 特許請求の範囲

主装置が乱数 R_n 又は R_n を含むデータを送り、カードで加工ののうち主装置に戻す α 環状路と、カードが乱数 R_e 又は R_e を含むデータを主装置に送り、主装置で加工ののうちカードに戻す β 環状路を併設したICカードシステム。

3 発明の詳細な説明

本発明は、カードの改ざんや偽造、主装置の不正作成使用を防止するICカードシステムに関する。従来のICカードシステムでは、使用中のカード端子から盗聴等を得た信号を記録し、うちにこの信号を再利用する不正使用への対策がなかった。本発明は、ICカードシステムに、主装置が乱数 R_n 又は R_n を含むデータをカードに送り、カードで加工ののうち主装置に戻す α 環状路と、カードが乱数 R_e 又は R_e を含むデータを主装置に送り、主装置で加工ののうちカードに戻す β 環状路を併設する。たとえば、主装置に発生させた乱数 R_n を交換又

は少くとも R_n を含む1組の値を全体変換した信号 S_1 をカードへ送り、カードが S_1 から復元した R_n 又は復元 R_n にもとづく変換値を信号 S_2 又は S_2' として主装置に返送し、さらにカード内に発生させた乱数 R_e を交換又は少くとも R_e を含む1組の値を全体変換した信号 S_3 又は S_3' を主装置へ送り、主装置が、復元した R_e 又は復元 R_e にもとづく変換値を信号 S_3 としてカードに返送する、ICカード、主装置、及びそれらより成るICカードシステムを構成する。

α 環状路は、主装置からカードに信号 S_1 を送る往路と、カードから主装置に信号 S_2 を返す復路と、 β 環状路は、カードから主装置に信号 S_3 を送る往路と、主装置からカードに信号 S_3 を返す復路を持つ。 α と β を独立に構成する他、 S_2' と S_3' を S_2 にまとめた、一部共有の構成も可能である。

β 環状路の復路信号 S_3 を用いた照合結果にメモリゲート駆動を行う構成とする。また、 α 環状路についてはカード内に2行う変換処理の結果が、 β 環状路については主装置内に2行う変換処理の

結果が、それと相反される復路信号とする。よって、復路信号と往路信号と異なるデータ形式に構成する。さらに、信号に複数の情報を混載しうる。例えば、往路の往路信号 S_1 にて、乱数 R_n の他に暗証 I やその変換 IU はじめ、パスワードやファイルキー、口座番号など f コードを混載できる。この際送信中の盗聴解読防止のため、複数の情報の合体変換加工を行う。ある環状路で運んだ f 等を、他の環状路に入力して処理、照合、同期等に用いる構成も可能である。

オ1図は本発明のICカードシステム構成図にて、少なくともIC外部からのアクセス不能メモリ⑬や制御プログラム⑭とCPU⑮をもつ主回路①を設置した、端子⑭つきICカード②及び、当該ICカードとデータ読み込み及びデータ処理を行う主装置③より、ICカードシステムが構成される。主回路①は、ワンチップIC又は数個のICにて実現する。主装置③は、少なくとも外部からのアクセス不能メモリ⑭や制御プログラム⑮とCPU⑯をもつ主回路④を

り、主装置に送る。 S_2 のフォーマットを $f_s R_e R_n W$ にて示す。 f_s , R_e , R_n の順序は任意でよく、また f_s は省略してもよい。主装置内にて、逆変換 W^{-1} ⑲が復元 R_n ⑳と復元 R_e ㉑を復元分離する。照合部⑳は㉒と、もとの乱数 R_n ㉓と比較照合し、不台致㉔なら排除し、台致㉕ならカードを正当と判断して㉖を交換 X ㉗に送るのを許可する。㉗は㉒と、 f_s 格納部㉘より取出したコード f_s ㉙とを合体変換加工して信号 S_3 ㉚をつくり、カードに送る。 S_3 のフォーマットを、 $f_s R_e X$ にて示す。 f_s , R_e の順序は任意でよく、また f_s は省略もできる。

カード側にて、逆変換 X^{-1} ㉛が S_3 ㉚から復元 R_e ㉜を分離し、照合部㉝にて㉜と、もとの乱数 R_e ㉞と比較照合の上、台致㉟すればメモリゲート㊱をオープンし、メモリゾーン㊲へのアクセスを許可する。

このように、カード側の照合部⑯にて復元 IU ⑭を検査するので使用者と主装置の両方の正当性をカードが判定でき、一方主装置側では、も

塔載する。主回路④はワンチップICや複数個のICをアセンブルしてブラックボックス化した集合体にて実現する他、主回路の代用として別のICカードを組み込んで用いることもできる。

オ2図は、本発明の実施例の処理の流れを示す。キー入力部⑤より入力の時証 I ⑥を交換 U ⑦にて IU ⑧に変換のち交換 V ⑨に入力する。⑨は主装置内の乱数発生部 Q_1 ⑩で発生させた乱数 R_n ⑪と IU ⑧とを合体変換加工して信号 S_1 ⑫をつくり、カードに送る。 S_1 のフォーマットを IUR_nV にて示す。 IU と R_n の順序は任意でよい。カード内にて、逆変換 V^{-1} ⑬が復元 IU ⑭と復元 R_n ⑮を復元分離する。照合部⑯は⑭と、識別データ格納部⑰より取出した識別データ IU ⑱と比較照合し、不台致㉑なら排除し、台致㉒なら使用者と主装置が正当と判定して㉓を交換 W ㉔に送るのを許可する。㉔はカード内の乱数発生部 Q_2 ㉕で発生させた乱数 R_e ㉖と、 f_s 格納部㉗から取出したコード f_s ㉘とを合体変換加工して信号 S_2 ㉙をつ

の R_n に対し主装置及びカードにて変換と逆変換をくり返した結果に得る R_n を主装置に還流させ、もとの R_n と比較照合することで、カードの正当性を判定できる。

上記にて、もしカード内で発生させた乱数 R_e を用いず、主装置がカードに R_e を含め信号 S_2 を送る構成とすると、信号の盗聴再利用を許してしまい不都合である。たとえばカードを正常使用中に端子から S_1 と S_2 信号を盗聴記録しておき、やちに正当でない主装置を用いて盗聴した S_1 信号をカードに入力すれば不正にカードを起動でき、カードより送られる S_2 や S_3 信号をよみとばして、盗聴した S_1 信号を入力すれば、不正の主装置にてメモリへのアクセスが可能としてしまい、他人や自分自身のカードの顔面改ざん等を可能としてしまう。

そこで、カードにて R_e を発生させ、 R_e 又は少くとも R_e を含む値の変換値をカードから主装置に送り、主装置は受けた R_e の変換値又は少くとも R_e を含む値の変換値を信号 S_3 としてカードに返送し、カードにて復元した R_e と、もとの発信した R_e と比較

照合して合致時にのみメモリゲートをオープンするよう構成すれば、主装置がたしかにカードから先刻発信された Re にもとづき S_2 を作成したと確認できる。よって、盗聴しおいた S_2 をカード入力しても、使用した Re 値がその都度異なるため、照合は成立せず、メモリアクセスできない。即ち、信号の盗聴再利用を防止できる。

合体変換する信号は、送信途上での盗聴防止のためであり、さらに複数個のデータをからめあわせて送ることと互にカラムフェーズすると共に一度に送信できるゆえ、カードと主装置間の送受信回数を減少できる。合体変換した結果のフォーマット、例えば $f_5 Re R_n W$ という表示は、 f_5 と Re 、 R_n といったコードや値を、手順 W を用いて変換処理した出力を示す。一例として

```
f5  01010011
Re  11010110
Rn  10101110
```

とし、 W 手順を

① f_5 とビット反転

識別データとして IU のかわりにパスワード等 f_4 を暗証入力 I と組合せを用いる際は、図3に示すように構成し、信号 S_2 のフォーマットを $f_4 I R_n V$ とすればよい。

図4図に信号のフォーマット例を示す。図4図(a)にて S_2 のフォーマットは $f_4 I U R_n V$ あるいは $f_4 I R_n V$ 、 S_2 の値は $f_5 R_n W$ となる。 $W=V$ 、 $f_5=f_4$ も可能である。 S_2 の値は $f_2 Re$ あるいは $f_2 Re Y$ となり、 Y は変換を示す。 $Y=V$ 、 $Y=W$ も可能である。 f_2 は省略できる。

S_2 のフォーマットは $f_2 Re X$ であり、 f_2 は省略できる。

図4図(b)は、 Re と R_n と I と U の信号内に組込を構成の例で、 S_1 、 S_3 のフォーマットは図4図(a)と同じであるが、 S_2 の値は $f_5 Re R_n W$ となる。

$W=V$ 、 $f_4=f_5$ も可能である。

⑤が α 環状路、⑥が β 環状路を示す。

⑤は選送し復元した f_5 、例えば口座番号等である。

② Re の上4ビットと、④を施した f_5 の下4ビットを交換

③ R_n の上4ビットと、 Re の下4ビットを交換

⑤ R_n の下4ビットと、④を施した f_5 の上4ビットを交換

⑦ 以上の順に2進した3バイトを合体して信号 S_2 とする

とすれば、 S_2 は 16進表示で EDCACA が生成される。さらに、 f_5 のバイト数を増加させ、秘密度を高める。又、 W^{-1} 手順は、上記 W 手順の逆プロセスとなる。

主装置に設けた変換 U は、主装置が不正目的で盗まれたり、秘密が洩れた時の暗号更新を円滑に行うための構成で、主装置を更新する際は変換 U

⑦を更新するのみでよい。カード使用者には、先ず本人確認のうち、入力された I と S_1 とに新 IU を作成して識別データ格納部⁽¹⁸⁾を更新するのみでよい。

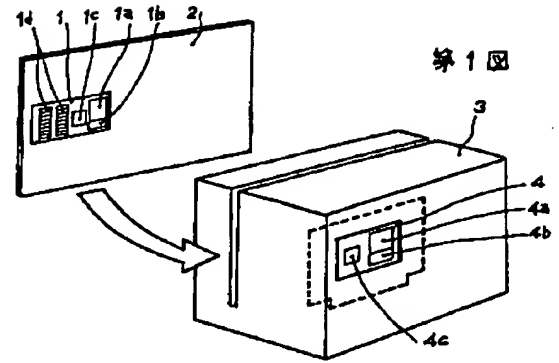
f には、パスワード、ファイルアクセスキーや他任意の値、コードを採用する。

4 図面の簡単な説明

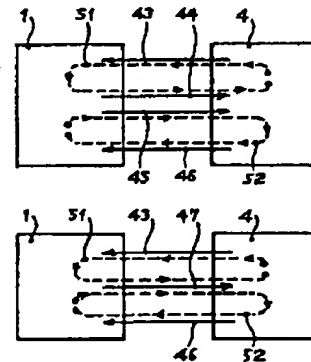
図1図は本発明のカードシステムの構成図、図2図と図3図は実施例の処理のながれを、図4図は信号のフォーマットを示す。

- 1...カードの主回路、1a...外部からアクセス不能メモリ、1b...制御プロケラム、1c...CPU、1d...端子、2...ICカード、3...主装置、4...主装置の主回路、4a...外部からアクセス不能メモリ、4b...制御プロケラム、4c...CPU、5...キー入力部、6...暗証 I 、7...変換 U 、8... IU 、9...変換 V 、10...乱数発生部 G_1 、11...乱数 R_n 、12...信号 S_1 、13...逆変換 V^{-1} 、14...復元 IU 、15...復元 R_n 、16...照合部、17...識別データ格納部、18...識別データ IU 、19...不合致、20...合致、21...変換 W 、22...乱数発生部 G_2 、23...乱数 Re 、24... f_5 格納部、25...コード f_5 、26...信号 S_2 、27...逆変換 W^{-1} 、28...復元 R_n 、29...復元 Re 、30...照合部、31...不合致、32...合致、33...変換 X 、34... f_2 格納部、35...コード f_2 、

36...信号 S_3 , 37...逆変換 X^{-1} , 38...復元 RE ,
 39...照合巻, 40...合致, 41...メモリゲート,
 42...メモリゾーン, 43...信号 S_4 , 44...信号 S_4' ,
 45...信号 S_4'' , 46...信号 S_5 , 47...信号 S_5 ,
 48... f_4 格納巻, 49...コード f_4 , 50...信号 S_4
 51... α 環状路, 52... β 環状路
 53...復元 f_5

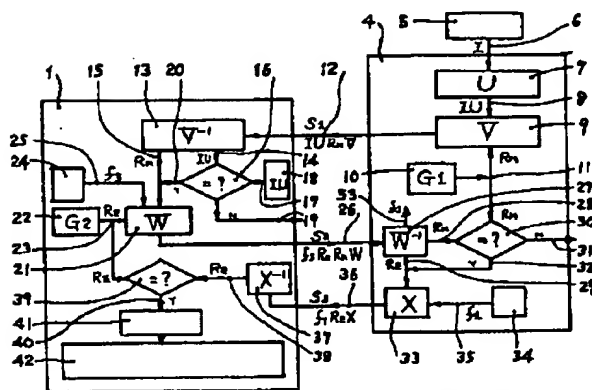


第1図

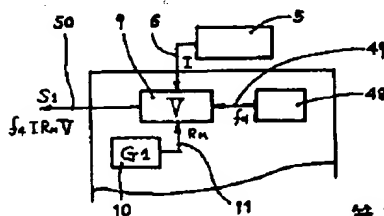
第4図
[a]

[b]

特許出願人 横江川 光



第2図



第3図

手続補正書

昭和62年11月10日

特許庁長官
(特許庁審査官)

殿
(殿)

1. 事件の表示

昭和61年

特許 願 第 188186 号

2. 発明(考案)の名称

ICカードシステム

送受に係る物品

指定商品および商品の区分

第 一 類

3. 補正をする者

事件との関係

特許 出願人

住所

郵便番号 122-0000

東京都千代田区東船場 2-5-2-401

氏 名 (法人にあっては代表者および
代表者の明を記すもの)

横江川 光

4. 補正命令の日付

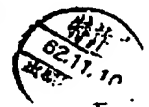
昭和 62 年 11 月 10 日

5. 補正の対象

明細書の発明の詳細な説明欄

6. 補正の内容

別紙のとおり



補正の内容

- 1 オ8頁 オ19行目
「 f_1 には、」とあるを、
「 f_1 や f_5 などには、」に補正。
- 2 オ10頁 オ20行目 ✓
「34... f_2 格納着」とあるを、
「34... f_1 格納着」に補正。
- 3 オ8頁 オ20行目の後に以下を挿入。
「いま S_1 と S_2 の往復にて、主記憶と使用者が正当と確定できたとして、例えばカードのメモリーゾーン④にデータを書きこみたいとき、カード側に書き込みを告げるコード f_1 ⑤を用いるが、このとき対象のアドレスや書き込むべきデータなどを f_1 に添え又は連結して f_1' とし、 $f_1' R_0 X$ のフォーマットの S_3 をカードに送り、カードが X^{-1} ⑦にて R_0 ⑧を復元時に f_1' も復元しておき、 R_0 照合合致④の α を f_1' を処理して書き込み

実行させればよい。このとき、複数個の S_3 を発信することと告げる f_1 を用いた S_3 を1個、先ず発信し、ついでデータを f_1 としてのせた S_3 を告げた個数だけカードに送ることにて、多量のデータを一挙にカードに送りこめる。

カード側にて書き込みが正常に完了すれば、それを通知するコード f_5 を再び S_2 の発信にて、主記憶側に通知することもできる。即ち、信号のやりとりは S_1 、 S_2 、 S_3 、 S_2 と続き、このように α 環状路と β 環状路を何度もくり返して交信ができる。この一連の交信時に、同一の R_0 や R_1 を用いてもよく、又例えば1回の交信毎に異なる乱数を用いてもよい。このとき、 S_3 のフォーマットとして S_2 のフォーマットと類似の $f_1 R_0 R_1 X$ を用いれば、1回毎に異なる乱数による α 、 β 両環状路の連続交信が可能になる。カードのメモリーゾーン④からの多量データを読み出しも、この α 、 β の連続にて授受できる。」

手続補正書

昭和63年3月1日

- 特許庁長官 殿
(特許庁審査官 殿)
1. 事件の表示
昭和61年 特許 願 第188186号
 2. 発明(考案)の名称 ^{フリガナ} ICカードシステム
 3. 補正をする者
事件との関係 特許 出願人
住所 郵便番号 122-00 〇〇
東京都足立区東綾瀬2-5-2-401 03-606-7103
^{フリガナ}氏 名 (法人にあっては代表者および
代表者の名を附けてその氏名) 横江川 光雄
 4. 補正命令の日付 昭和63年2月2日
 5. 補正により増加する請求項の数
 6. 補正の対象 昭和62年11月10提出の特許補正書の「補正の対象」の欄
 7. 補正の内容 別紙のとおり

手続補正書

昭和62年11月10日

- 特許庁長官 殿
(特許庁審査官 殿)
1. 事件の表示
昭和61年 特許 願 第188186号
 2. 発明(考案)の名称 ^{フリガナ} ICカードシステム
 3. 補正をする者
事件との関係 特許 出願人
住所 郵便番号 122-00 〇〇
東京都足立区東綾瀬2-5-2-401
^{フリガナ}氏 名 (法人にあっては代表者および
代表者の名を附けてその氏名) 横江川 光雄
 4. 補正命令の日付 昭和 年 月 日
 5. 補正により増加する請求項の数
 6. 補正の対象 明細書の発明の詳細な説明の欄
明細書の図面の簡単な説明の欄
 7. 補正の内容 別紙のとおり